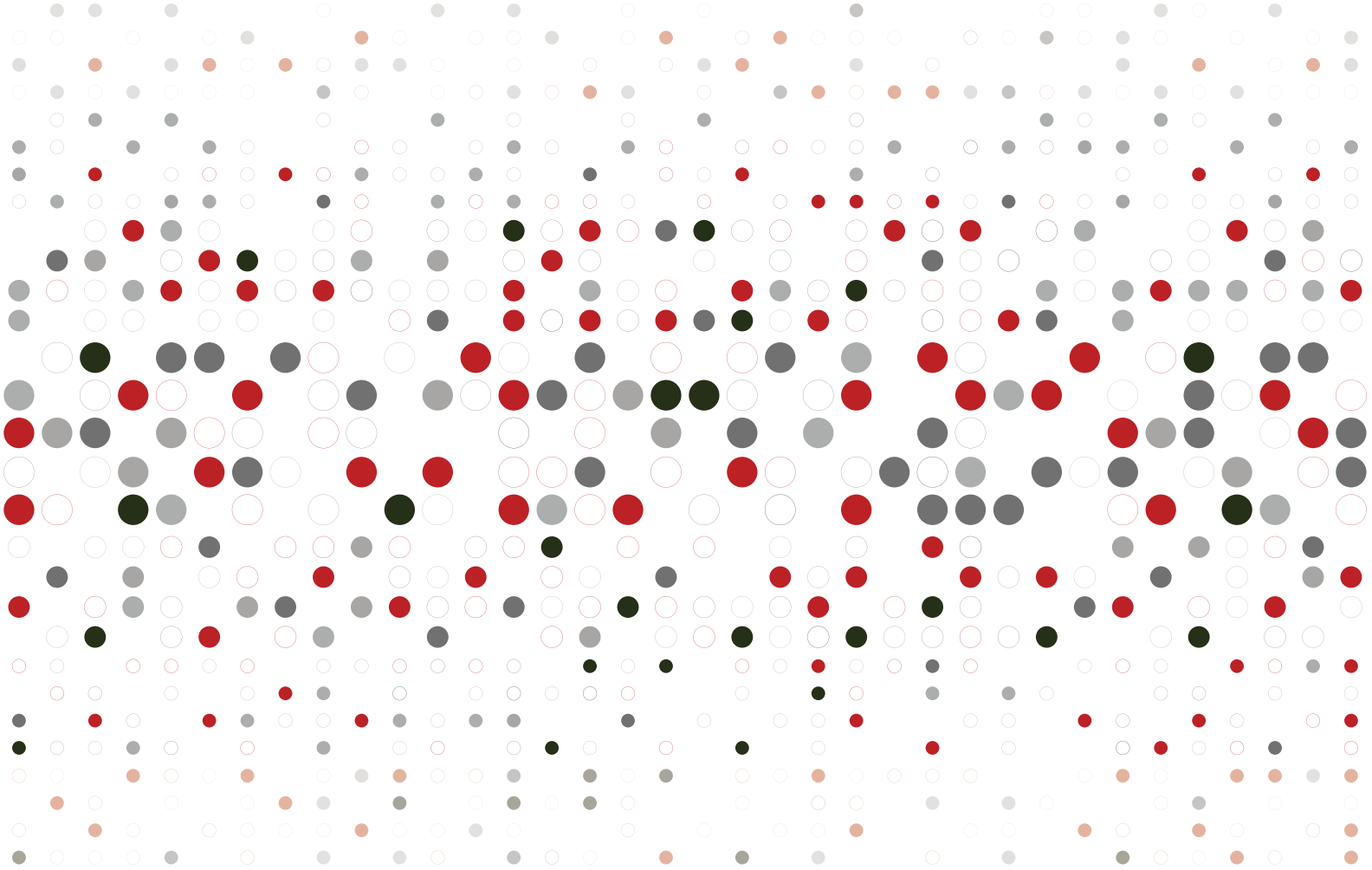
BLOCKCHAIN
AND INTERNAL AUDIT

A joint research report by the Internal Audit Foundation and Crowe

By Richard C. Kloch, Jr., CPA and Simon J. Little, CPA



Crowe

INTERNAL AUDIT FOUNDATION™

Published by the Internal Audit Foundation
1035 Greenwood Blvd., Suite 401
Lake Mary, Florida 32746, USA

The IIA’s International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and the Foundation work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today’s business world. Much of the content presented in their final reports is a result of Foundation-funded research and prepared as a service to the Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or the Foundation.

ISBN-13: 978-1-63454-065-0
23 22 21 20 19 1 2 3 4 5 6

Table of contents

Introduction and executive summary

The growing popularity of blockchain networks, coupled with blockchain's potential to fundamentally transform the way many business processes are handled, raises an important question for internal auditors: What steps, if any, should the profession be taking in response to this transformational technology?

A blockchain (a type of distributed ledger) is a shared database that creates a permanent record of transactions. The database is shared across a network of multiple connected devices, which are known as "nodes." Whenever a new transaction is added to the ledger, the update is immediately viewable by all the other nodes on the network. In addition, the transactions – or blocks – are structured in a way that is designed to make it impossible to go back and change a previous entry.

Blockchain's initial prominence arose from its use as the underlying technology for powering digital currencies such as bitcoin. But the technology has numerous other applications in a variety of business processes and entities beyond cryptocurrencies. As these applications become more widespread and commonplace, internal audit's role as the third line of defense in risk management will be directly affected.

Certain attributes and features of blockchain technology open up the possibility of numerous new and promising applications in a broad range of industries, from financial services to healthcare, from software development to manufacturing and food production – and many more. Yet, in many ways, enterprisewide blockchain applications are still emerging. Evidence suggests that while some internal audit departments are responding to blockchain adoption by their companies, the profession as a whole has not yet taken a leading role in this area.

To be sure, some of the largest organizations in industries in which blockchain offers the most obvious promise are taking actions to address audit challenges associated with this technology. Yet because the record of blockchain transactions is supposed to be unalterable, and because blockchain transactions are immediately visible to all participants, there has been, to varying degrees, a misconception that the need for assurance activities related to blockchain is limited.

However, most internal audit professionals ultimately will be directly and significantly affected by blockchain technology. Even if their organization does not choose to embrace blockchain, their suppliers, customers, or other third parties likely will adopt blockchain processes such as smart contracts, which will make it necessary for them to address the technology in order to take part in transactions. At a minimum, internal auditors will need to develop a working knowledge of the functions and risks of the technology. Internal audit professionals will likely be called upon to leverage new methods and tools for validating blockchain networks' structure and viability, for evaluating the effects blockchain transactions will have on their organizations' risk exposures, and for assessing the appropriateness and effectiveness of the risk mitigation efforts associated with blockchain transactions.

This research report is intended to provide internal auditors in various types of organizations with a basic framework for assessing their current level of blockchain technology preparedness and to provide them with a road map for developing audit plans that address blockchain issues as they are encountered.

The immediate objectives are to help readers understand specific risks and threats and to help them begin to prepare for blockchain adoption so that proper controls can be developed and implemented. Ultimately, the development of such knowledge could also provide internal auditors with additional opportunities to add value to the activity within their organizations by becoming recognized sources of blockchain proficiency.

1) The relevance of blockchain

A blockchain type of distributed ledger differs from other types of shared databases in several important ways. One of these distinguishing characteristics is its capability for creating a permanent record of transactions that are designed to be unchangeable. Whenever a new transaction is added to the ledger, the update is immediately viewable by all other nodes on the network.

This structure also makes blockchain networks transparent and resilient. They are transparent because no participant can make any changes to an existing entry (or block), and they are resilient because the failure of a single node (or even a group of nodes) will not cause data to be lost. Such features have obvious value in situations in which a single, shared, and unalterable version of the truth is needed.

Blockchain and other technologies

As part of what's known as the "fourth industrial revolution," digital technologies such as artificial intelligence, machine learning, robotic process automation, advanced data analytics, additive manufacturing (or 3D printing), and the internet of things (IoT) have the potential to revolutionize many business processes – and even entire industries. But the individual impact of each technology can be multiplied when it is combined with other types of digital technology.

For example, IoT-connected devices allow healthcare providers to monitor patient conditions remotely, in real time – an important advance. But what makes these IoT capabilities even more viable is an underlying blockchain infrastructure that can also verify the IoT sensors are producing valid, authentic information with which no one has tampered.

Such a fusion of digital technology has the potential to create entirely new business models by enabling interoperability, machine-to-machine communication, and new cyberphysical systems. In some instances, such fusion can create new revenue opportunities. In most instances, it creates the opportunity for greater efficiency by allowing existing transactions to be done faster and at lower cost.

A fluid and evolving risk environment

As intriguing as these technological advances are, their transformative and evolving nature presents particular challenges for internal auditors. No two organizations approach these capabilities in the same way, and no organization is likely to operate using blockchain-based technology exclusively. Blockchain applications will interface with more conventional processes at various points and in various ways.

These widely varying scenarios mean internal audit will need to adjust to varying degrees of interaction and complexity involving numerous digital technology applications. To do that, internal audit will need to develop resources with expertise in multiple types of technology and will need to create a collaborative environment that is capable of adapting quickly as blockchain continues to evolve.

2) Adoption of blockchain technology

It is not necessary to fully grasp all the technical workings of blockchain to recognize both the potential benefits and the challenges it can present to internal audit, but it is helpful to have a basic understanding of a few fundamental concepts as described here.

Public and private blockchains

As noted in the preceding section, a blockchain is a shared database or ledger that is distributed across a number of nodes in a network of computers. A blockchain network can be open to the public or private, with only select participants.

Each blockchain type offers varying degrees of the type of actions users can take. Certain situations offer "permissionless" access, which allows users to read, write, and validate transactions. Permissionless access is commonly used in public networks, such as those that enable the exchange of cryptocurrencies.

Other situations offer "permissioned" access, which limits the possible actions of certain or all network participants. Permissioned access is more commonly associated with private blockchain networks. Most enterprise blockchains (those used by companies for noncrypto purposes) are private, permissioned blockchains.

A private blockchain is established by an organization or group of organizations that agree to participate in the shared ledger – such as a large manufacturer and its various suppliers, a holding company and its subsidiaries, or a payment processing network and its participating member companies. The company or consortium that establishes the network administers it and controls access.

Private blockchain networks offer a number of benefits that can be of significant advantage to many types of enterprises. Blockchain networks establish trust among the ecosystem participants and consumers through several different methods. Blockchain provides all involved parties transparency into the processes, inputs, procedures, and other aspects of a process or function. This transparency can extend throughout an entire process, from raw material producer to the consumer. Also, transactions that are added to a blockchain are validated not by human input that can potentially be influenced or corrupted, but by impartial mathematics spread among multiple nodes, which confirm a transaction's adherence to preestablished conditions.

Smart contracts

Blockchain executes transactions using business processes that have been developed as software code and are referred to as smart contracts. Smart contracts can require that a specific contract term or milestone must be met before the next transaction can take place. They also make it possible to automate the monitoring and enforcement of contractual promises with minimal human intervention, resulting in greater efficiency and improved opportunities to scale up operations with less additional investment.

In financial services, for example, certain types of commercial lending to finance inventory traditionally have been constrained by the need to perform on-site audits and physically validate sales records and inventory. With blockchain technology, lenders can use smart contracts to enforce loan terms and automate the sales verification process. This capability reduces the costs and constraints of performing physical audits, and it also significantly reduces the potential for fraud.

In addition to reducing costs by automating manual and paper-based tasks, blockchain increases the speed of work processes by significantly reducing the use of intermediaries and the need for manual verification. This capability is already being demonstrated in the payment processing industry, in which large banks have begun using blockchain to cut costs and dramatically accelerate the settlement time for global payment transactions.

Illustrative blockchain applications

In mid-2018, one online researcher and blockchain advocate compiled a list of more than 200 large banks and other financial services businesses worldwide that were either using or exploring blockchain applications at that time[1] – a list that has undoubtedly continued to grow. Blockchain can allow banks and other financial services providers to share and automatically update customer information among all business units, which can improve the customer experience and reduce customer acquisition costs.

Blockchain also offers the capability to improve other business functions, including sales, marketing, and regulatory compliance. Other use cases in financial services for blockchain include new applications for processing international payments, accelerating the clearing and settlement processes in securities trading, and processing trade finance transactions.

Outside of financial services, many other industries are also actively developing new use cases for blockchain technology. In healthcare, for example, large providers are exploring ways to use blockchain to ensure both the privacy and accuracy of patients' electronic medical records as well as medical billing and claims processing. One of the largest insurance companies in China has begun partnering with more than 100 hospitals to use blockchain technology to securely process patient data and financial information.[2] In the United States, a leading retail chain has been awarded a patent for a system designed to store patient medical records via blockchain.[3]

Looking beyond health insurance alone, the broader insurance industry is exploring blockchain applications across a wide variety of operational functions, including claims handling, subrogation, and reinsurance. The technology research company ReportLinker projects the global blockchain insurance market is likely to grow from an estimated $64.5 million in 2018 to a projected $1.4 billion by 2023 – a compound annual growth rate of nearly 85 percent.[4]

Blockchain also is garnering considerable attention in manufacturing and distribution operations involving the production and movement of physical products. Smart contract applications can enable the automation of many routine supply chain management processes, using blockchain to digitize information and then track the origins and history of goods and materials.

In August 2018, a group of 10 large food companies announced an initiative that uses blockchain ledgers to improve food safety by enabling immediate traceability of produce and commodities in the food chain.[5] Beyond merely tracking the handling of shipments and transactions, blockchain offers even greater potential benefits when it is coupled with other advanced technology systems, such as water testing mechanisms, sensors, and precision delivery systems for pesticides and water, which can be connected via an IoT network that interfaces with the blockchain ledger.[6]

While the challenges can be significant, the fast-growing number of viable use cases suggest the potential rewards of adopting blockchain technology can be dramatic – and in many instances could be downright transformative. In view of this, the internal audit profession should ask this question: What will be the role of internal auditors as this technology advances, and how can the profession adapt to provide the greatest value to sponsoring organizations?

3) Challenges for internal audit

Although there do not appear to be any specific blockchain use cases that have been developed for applying blockchain to the internal audit function itself, internal auditors nevertheless have a significant role to play in blockchain development. Internal audit's function will need to evolve to encompass the ability to validate that the individual components of a blockchain are functioning correctly. This process includes validating access permission, encryption, and cryptographic code, as well as reviewing the validation of smart contract transaction codes, functionality, and security. The relevant governance, risk management, and control procedures also will require internal audit consideration.

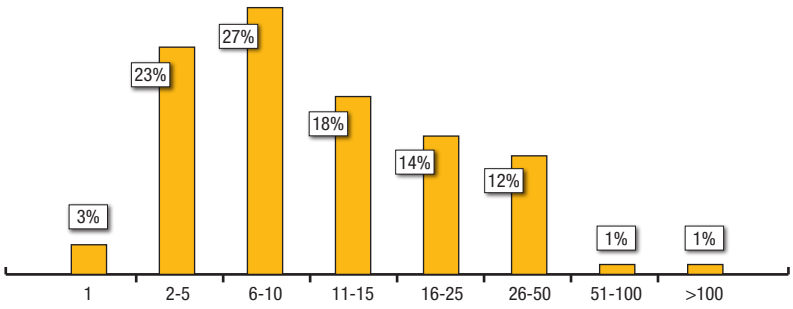
Current awareness and understanding

In order to gauge the profession's general preparedness for this evolution, The Institute of Internal Auditors' (IIA's) Audit Executive Center, in collaboration with the Internal Audit Foundation and Crowe, conducted a limited survey of IIA members. The survey participants represented organizations of various sizes, including both privately held and publicly traded companies and public sector and not-for-profit organizations. There was significant representation from the finance and insurance, manufacturing, educational services, transportation, and public administration sectors.

As shown in Exhibit 1, the internal audit operations represented by the survey respondents encompassed a broad range of sizes and sophistication, ranging from single-person operations to large departments of more than 50 employees. Departments with between six and 10 people made up the largest segment of the survey population.

Exhibit 1: Survey participants' internal audit departments

What is the size of your internal audit function?

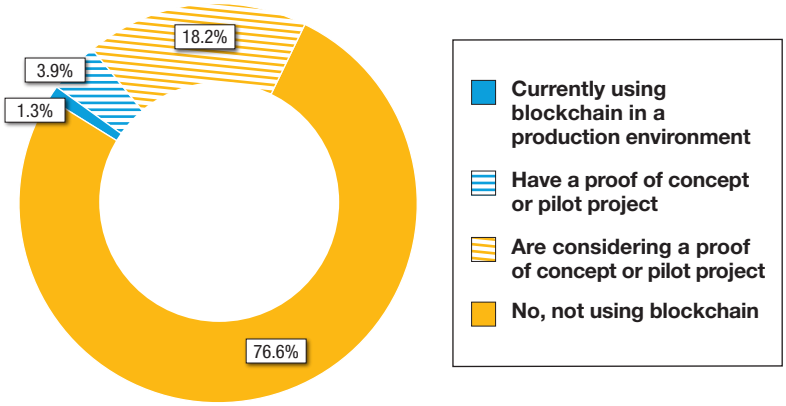


Source: IIA Quick Poll, December 2018
Note: Due to rounding, the percentages do not total 100.

The survey responses raised significant questions about the profession's readiness for the potentially transformative effects of blockchain technology. For example, when asked if their organizations were already using blockchain in a production environment, or whether they currently have or are considering developing a proof of concept or pilot project of blockchain technology, three-quarters of the respondents were not aware of any such preparatory activities in their organizations. (Exhibit 2)

Exhibit 2: Current blockchain involvement

Is your company using blockchain, and if so, how?



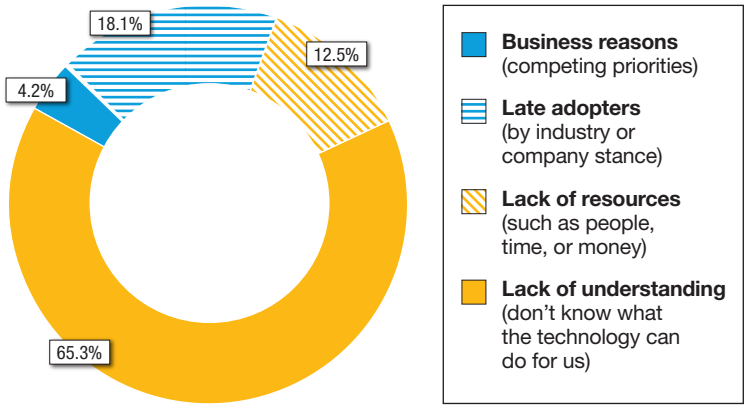
Source: IIA Quick Poll, December 2018

It is possible, of course, that at least some of the organizations represented by "no" responses actually have begun blockchain development, but the respondents were simply unaware of it. In either case, however, the high number of "no" responses suggests that the majority of the internal audit professionals surveyed have little or no familiarity with potential blockchain applications in their organizations.

This impression is reinforced by the participants' responses to another question. When asked to describe the greatest impediment to blockchain adoption in their companies, survey respondents were allowed to provide open-ended, unscripted responses. When the unscripted responses were analyzed and categorized, the majority of the responses described a basic lack of understanding, revealing that decision-makers did not know or understand the technology or recognize what it could do for them. (Exhibit 3)

Exhibit 3: Obstacles to blockchain adoption

What is the largest obstacle to considering or adopting blockchain technology?



Source: IIA Quick Poll, December 2018
Note: Due to rounding, the percentages do not total 100.

The lack of understanding indicated by the IIA poll is not altogether surprising, given that blockchain technology is still in its emergent phases. In many instances, companies have not yet seen a reason to adopt or learn about the technology, because adoption in their industries has not been visible enough to make it a high priority.

Acceptance followed by adoption

Some industry observers have compared the state of blockchain today with the state of the internet in the early 1990s.[7] In its infancy, the internet was regarded as an interesting novelty, rather than the revolutionary tool it has become. Moreover, when companies began to go online, their initial focus was on corporate intranet applications – quite often, employee access to the web, email, or other outside resources was either prohibited or severely restricted.

As internet access became more useful, and as IT security protocols became more sophisticated, these limitations gradually were lifted. Eventually, internet access became more than just useful – it became essential. Businesses today depend on cloud solutions to conduct some of the most critical aspects of their business operations, and they use cloud storage for their most sensitive records and documentation. The same pattern – doubt, followed by limited acceptance and participation, culminating in widespread adoption and proactive usage – is seen by many as a likely scenario for blockchain's future.

As the technology gains wider mainstream acceptance and greater relevance, and as blockchain ledgers begin to handle more business, both in terms of the number of transactions and their dollar value, it will become increasingly important for organizations to develop comprehensive policies and procedures that incorporate blockchain protocols and best practices. That means internal audit will need to develop procedures to assess the performance of blockchain systems. It also will be necessary for internal auditors to update their understanding of both the internal and external risks associated with blockchain processes, and to develop relevant monitoring procedures.

4) Preparing for blockchain adoption

Regardless of the specific applications that are launched, the adoption of blockchain requires far more than technological expertise alone. For most organizations, the first step is to verify whether blockchain is indeed the most appropriate solution for the particular issue being addressed. To make the business case for blockchain, proponents must be able to demonstrate why blockchain would be preferable to using a traditional database for the function in question. Further, they must be able to demonstrate potential cost savings, revenue enhancements, or measurable improvements to other critical business metrics.

Internal audit's input and involvement at this stage would focus primarily on concerns related to governance, security, audit policies and procedures, and other risk management and control issues. In addition, internal audit should be thinking about the strategy and business case for blockchain adoption in order to be able to offer relevant input.

The degree to which internal audit is involved in these issues will vary, depending on whether the organization is developing its blockchain internally or adopting the technology from third-party sources. These areas of focus can be organized into a framework composed of four major components:

Resources and human capital

The internal audit function should expect that blockchain adoption will necessitate some adjustments in terms of both human and organizational resources in order for internal audit to continue meeting its responsibilities. In addition to recruiting candidates with internal audit or accounting and finance backgrounds, some internal audit departments might want to consider expanding their recruiting efforts to include candidates with certain technical skills such as coding or cybersecurity, which is a relevant issue in blockchain adoption. Additionally, the use of outside firms with specialized skills can provide expertise in the absence of adequate individuals in the workforce.

Because blockchain use cases are often combined with other emerging technologies, no single mix of specialties is ideal for every organization. Nevertheless, a general orientation toward technology, particularly in areas such as advanced analytics, is likely to be an attractive trait for future internal audit professionals as business processes become increasingly automated.

In addition, of course, internal audit managers should continue looking for recruits with sound critical thinking and problem-solving capabilities and strong communication skills. Most internal audit departments already value these traits. Specialized training related to the specific blockchain application is also likely to be required, both for new hires and existing internal audit staff.

Risk identification

In any risk management effort, accurate and thorough identification of risks is an essential starting point, and this is certainly true when preparing for blockchain adoption. As is the case with so many other factors involving blockchain, the specific risks associated with the technology will vary from one use case to the next; however, several areas of risk would be applicable to almost all blockchain implementations. These include:

- **Client information security.** As mentioned earlier, protecting the confidentiality of personal health and financial information is a recognized area of regulatory risk in financial services and healthcare applications. In addition, the European Union's General Data Protection Regulation (GDPR) expands this protection to all types of personal information. In today's global economy, organizations of all sizes and types could find they have exposure to GDPR issues. Internal audit will have an important role to play in determining that existing confidentiality protections are adapted as necessary to accommodate blockchain adoption, while at the same time remaining in compliance with regulatory requirements.

- **Network complexity.** The inherent risk associated with a blockchain network can vary significantly depending on the number of nodes on the network, the presence or absence of backup nodes, and management judgment as to whether such backup systems are needed.

  A private blockchain composed of a dozen vendors in a supply chain presents a far different risk profile than a large healthcare blockchain containing the medical records of thousands of patients. In fact, a larger network can actually help reduce certain types of risk.

  For example, in a network of many thousands of users dispersed over a broad area, the risk of all nodes failing and causing a loss of data becomes miniscule. Nevertheless, low likelihood, high-impact risks are still important. Because of the extraordinarily high impact a network failure would have on a blockchain-based business process, this area of risk still must be addressed.

  Another related area of risk relates to the consensus algorithm that network participants have agreed to use to structure and record their transactions. This algorithm directly affects many other factors, including block structure, storage needs, and security risk.

- **Network model.** Public and private blockchains present distinctly different risk profiles. Private blockchains nearly always have fewer nodes than public blockchains. As more entities are added to a blockchain, the number of points at which the blockchain interacts with nonblockchain networks typically increases – as does the associated risk of security breaches or other vulnerabilities. Variations in these connected networks' security protocols add additional layers of risk exposure.

- **Smart contracts.** As smart contracts increase in complexity, with more participants, more detailed instructions, and more precisely defined contract milestones, the opportunity for error increases as well. One particular area of focus involves the system's interaction with "oracles" – that is, "off-chain" entities that are trusted providers of critical information.

  Consider, for example, crop insurance or some other type of parametric insurance, which does not indemnify policyholders against specific losses but instead agrees to make payment upon the occurrence of a triggering event, such as flooding or a hailstorm. These triggering events typically are verified by an independent, outside agency such as the National Weather Service. When such insurance is administered via a smart contract, the outside agency is referred to as an oracle – and any risks associated with the oracle's performance can become embedded in the blockchain as well.

  In other words, if the oracle introduces erroneous information, that error contaminates the entire blockchain. Identifying and quantifying oracle-related risks can easily become one of internal audit's most difficult risk assessment challenges.

- **Code.** The code that is used to write the blockchain software presents another area of risk that is specific to blockchain adoption. The use of recognized code development methodologies, coupled with validation that the code performs the necessary functions as required, can be useful in accurately identifying and quantifying this risk. The risk assessment should also take into account the potential for a malicious actor to infiltrate the contract code during development, implementation, or maintenance.

This list is only a starting point, encompassing just some examples of the risks associated with blockchain adoption. Indeed, the purpose of this discussion is not to produce an exhaustive risk identification checklist, but rather to point out certain types of risk that could be considered unique to blockchain technology. A more complete risk assessment in preparation for blockchain adoption would necessarily include the full spectrum of general technology-related risks, with particular attention to cybersecurity risk.

Control procedures

When a business implements a blockchain application, internal audit will need to evaluate the processes, risks, and controls related to that application. Internal audit does not necessarily define the controls, but it does need to review and test them, both to evaluate their adequacy and to validate they are being implemented as required.

Some of the specific control elements that need to be developed include:

- **Data.** In addition to understanding what types of data are recorded in each block of the chain, internal audit should also review the appropriate volumes (or throughput) and transaction speeds (or latency) for handling that data. For example, a credit card processor that handles millions of transactions a day will have vastly different requirements and control procedures than a manufacturer operating a private network of only a few dozen suppliers. Controls should also exist to verify that the consensus algorithm – the actual code that validates each ledger entry in the blockchain – is appropriate for the blockchain's intended purpose and is functioning as designed.

  Data privacy is a related area of concern, especially in industries such as financial services and healthcare, in which the privacy of personal information is a regulatory concern. The structure of individual blocks allows for data to be securely encrypted, but internal audit still needs to validate that such structures are in place, properly employed, and functioning.

  In any business process, handoffs or transition points between individuals or subprocesses are vulnerable to failure or errors. This is true in blockchain applications as well. The transition points where the blockchain interacts with other, conventional business systems require adequate controls.

- **Storage.** Because the amount of data that can be stored within each block in the blockchain can vary, this variable needs to be defined, with adequate controls put in place. In addition, basic data storage controls – either on-site or in the cloud – also must be established. Because a blockchain's distributed ledger is stored on multiple nodes – presumably in diverse locations – disaster recovery and business continuity issues are alleviated to some degree. Nevertheless, it cannot be said that such risks are eliminated completely. Internal audit will need to develop procedures for evaluating and validating basic data storage controls, as well as verifying that relevant business continuity plans and resources are in place.

- **Access.** Controlling access to the blockchain is a critical area of concern for both privacy and data integrity purposes. This concern is especially true for private or permissioned blockchains, in which a central administrator limits access to authorized users only.

  One way a blockchain maintains transaction security is by means of public and private keys – essentially large integer numbers that are represented using a series of letters and numbers. Public keys sometimes are compared to a bank account number, while private keys are comparable to the

password used to access the account. These keys must be encrypted and securely stored, with adequate control procedures that limit access. Most private blockchains are likely to grant different users varying levels of access permission, depending on their function. Again, each company or consortium will need to define the permission levels to meet its own requirements, but permissions and access are always areas of concern in any IT audit process. The adequacy and implementation of these access controls need to be evaluated and verified by internal audit.

Risk management and mitigation

Just as the preceding discussion should not be considered an attempt to produce a comprehensive risk identification framework, the risk mitigation points discussed here should be considered only a starting point for organizations launching a more complete and tailored risk management and risk mitigation program.

One of the most critical components of such a program revolves around cybersecurity. The introduction of blockchain technology also creates the need for additional cybersecurity enhancements. These include applying recognized cybersecurity practices to the validation of permitted nodes, as well as validating sound cybersecurity practices in developing smart contracts and managing the necessary external interactions that will be involved in the process.

Ideally, internal audit should have access to resources that are capable of evaluating the structure of blocks themselves to verify that they are indeed immutable and that necessary cryptography features, such as public and private keys and digital signatures, are functioning and secure.

At a high level, possible considerations for internal audit include:

- **Governance.** Governance includes issues such as private key security guidelines, definition of standard operations, procedures for adding and removing nodes, and various digital signature components and verification algorithms.
- **Risk management.** Risk management encompasses the specific risks discussed earlier, such as private key storage and security, smart contract monitoring for code errors and tampering, interaction with nonblockchain entities, and off-chain data storage.
- **Control procedures.** Control procedures include managing network access, specific network actions, node agreement, ordering and execution of transactions, and the maintenance of current block versions and content.

In addition to real-time smart contract monitoring, most organizations – particularly those that must answer to large groups of shareholders – will also require auditing and reporting on a regular basis to demonstrate that systems are functioning as intended. These activities also need to be incorporated into the long-term internal audit strategy and plan.

Conclusion

When blockchain technology first began expanding beyond the realm of cryptocurrencies, some observers questioned whether the day might come when financial audits and independent attestation would no longer be necessary because all transactions would be conducted on incorruptible blockchains. To a lesser degree, similar speculation emerged about the risk management duties of internal auditors. In both instances, it soon became clear that these conjectures were inaccurate.

To be sure, some of the work routinely performed by internal audit, such as reconciling differences between various ledgers or records, might appear to be redundant to the casual observer – after all, in a blockchain environment, participants are using the exact same ledgers. But, as recent successful hacker attacks on cryptocurrency networks have shown,[8] blockchain security is not infallible – a fact that calls into question other assumptions about the immutability and security of smart contracts and other blockchain applications.

As blockchain applications become more common, the responsibilities of the internal audit function actually are likely to expand in important ways. Internal audit will need to develop policies and procedures to validate the proper function of blockchain networks. It also will fall to internal audit to validate that ledger versions are updating properly at all nodes, that nodes are appropriately secured, and that the consensus algorithm is valid and consistently applied.

Such tasks will require a fairly significant level of technological expertise, either within the internal audit department or available from reliable outside providers. At the very least, existing IT project auditing skills will need to be enhanced and adapted through appropriate training in issues related to blockchain technology. Some software providers are already focused on creating technology for assessing oracle safety, for example, along with products that provide real-time monitoring of smart contract volumes in order to warn administrators of suspicious spikes or drops in activity. The ability to assess, select, and implement such software will very likely be yet another technical capability that the internal audit manager must look for when recruiting new talent or training existing personnel.

Although survey responses and industry interactions suggest many internal audit departments are not yet fully prepared for these dramatic changes, some large organizations are embracing this technology and finding real business benefit for the investment. As they do, the internal audit profession will find itself challenged to adapt quickly – but also invigorated by the opportunity to take a leadership role in helping their organizations absorb and apply this new technology.

[1] Mappo, "Comprehensive List of Banks Using Blockchain Technology," hackernoon.com, Aug. 20, 2018, https://hackernoon.com/comprehensive-list-of-banks-using-blockchain-technology-97c08fa88385

[2] Joseph Young, "Tencent and Alibaba's Insurance Giant Is Using Blockchain With 100 Hospitals," CCN.com, June 1, 2018, https://www.ccn.com/tencent-and-alibabas-insurance-giant-is-using-blockchain-with-100-hospitals

[3] Ana Alexandre, "Walmart Awarded Patent for Blockchain-Based Medical Records System," Cointelegraph.com, June 23, 2018, https://cointelegraph.com/news/walmart-awarded-patent-for-blockchain-based-medical-records-system

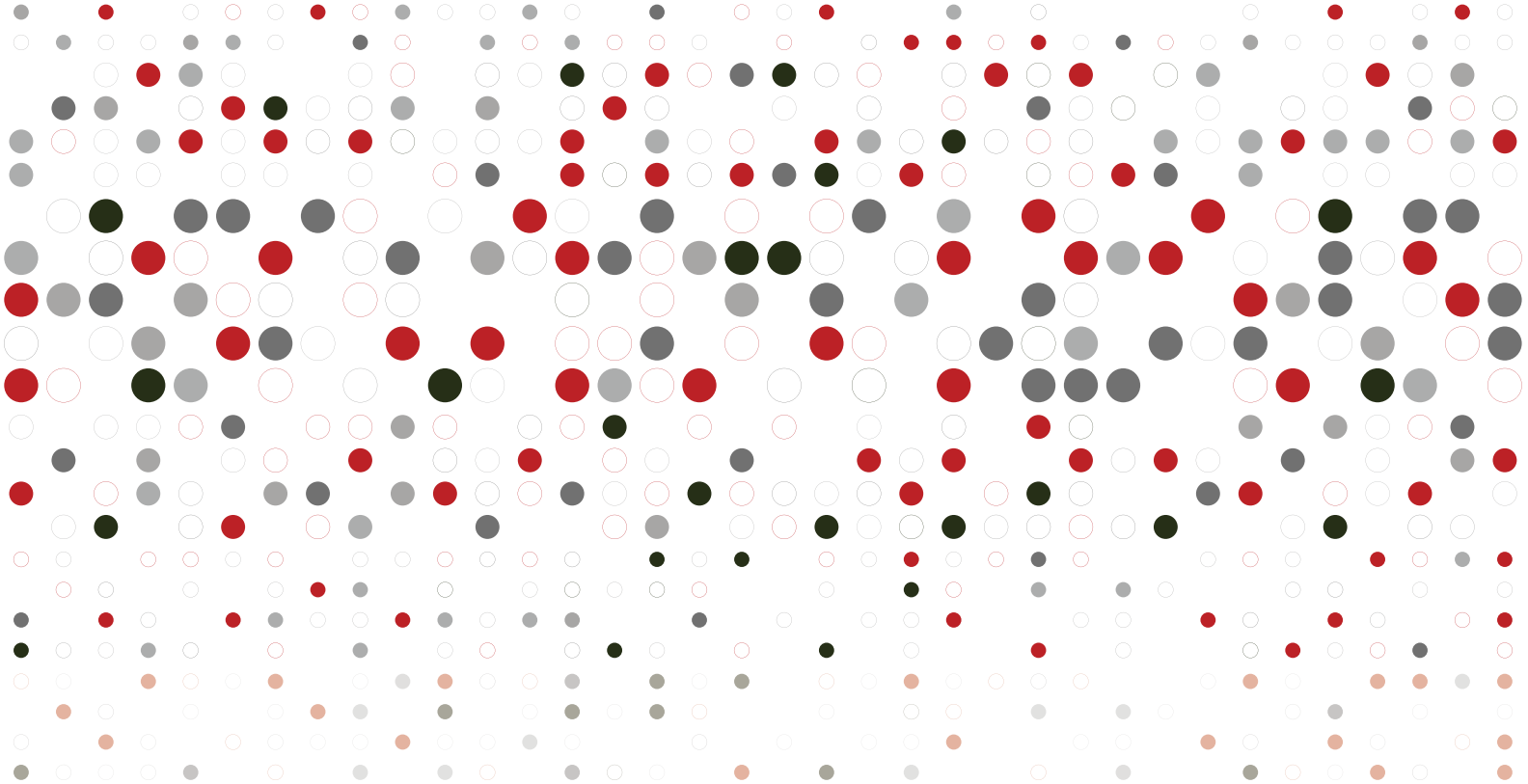
[4] "Blockchain in Insurance Market by Provider, Application, Organization Size and Region – Global Forecast to 2023," ReportLinker, July 2018, https://www.reportlinker.com/p05474768/Blockchain-In-Insurance-Market-by-Provider-Application-Organization-Size-And-Region-Global-Forecast-to.html

[5] "'Food Trust' Partnership Uses Blockchain to Increase Food Safety," ITU News, Aug. 21, 2018, https://news.itu.int/food-trust-blockchain-food-safety

[6] Jenny Splitter, "What Can Blockchain Really Do for the Food Industry?" Forbes, Sept. 30, 2018, https://www.forbes.com/sites/jennysplitter/2018/09/30/what-can-blockchain-really-do-for-the-food-industry/

[7] Joichi Ito, Neha Narula, Robleh Ali, "The Blockchain Will Do to the Financial System What the Internet Did to Media," Harvard Business Review, March 9, 2017, https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

[8] Mike Orcutt, "Once Hailed as Unhackable, Blockchains Are Now Getting Hacked," MIT Technology Review, Feb. 19, 2019, https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/



Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

RISK-19001-003K

Crowe

INTERNAL AUDIT FOUNDATION™

2019-2675